ABSTRACT

A system and method for facilitating BIOS integrated encryption is provided. An interface is defined between the operating system and the BIOS. The operating system employs this interface to provide BIOS code information to facilitate decryption of data that is encrypted on the system. In the pre-operating system boot phase, the BIOS employs the decryption information provided from this interface in order to decrypt the data. The decrypted information can be employed to facilitate secure rebooting of a computer system from hibernate mode and/or secure access to device(s).

5